Scan2Tray

# Incident Response Policy

**Scan2Tray Ltd** (Company No. 17096824) · Version 1.0 · 24 September 2026 · Owner: Paul Hinett, Director · hello@scan2tray.com
Supplement to the Scan2Tray Information Security Policy.

## 1. Purpose and scope

This policy defines how Scan2Tray detects, reports, handles and learns from security incidents affecting its systems, its sellers, their buyers, or marketplace partners such as TikTok Shop. It applies to all staff and contractors and to every Scan2Tray system, including the API, web, desktop and mobile applications, hosting, and marketplace integrations.

A **security incident** is any actual or suspected unauthorised access to, disclosure, alteration, loss or unavailability of Scan2Tray data or systems. Examples: a leaked credential or API key, a compromised staff device, a marketplace token used outside Scan2Tray, a data exposure bug, malware, a denial-of-service, or a supplier breach that touches our data.

## 2. Roles and responsibilities

| Role | Responsibility |
|---|---|
| Incident Lead — Paul Hinett, Director (security owner) | Owns every incident end to end: declares it, directs containment, decides on notifications, approves the post-incident report. Deputises a named engineer if unavailable. |
| Engineers | Investigate, contain and remediate under the Incident Lead's direction; preserve logs and evidence; do not communicate externally. |
| All staff and contractors | Report anything suspicious immediately (section 3). Reporting early is never penalised, even for false alarms or self-caused issues. |
| Communications | The Incident Lead is the single point of contact for sellers, marketplace partners, regulators and suppliers. |

## 3. Reporting and communication channels

- **Internal reporting:** immediately by phone or direct message to the Incident Lead, followed by email to **hello@scan2tray.com** with "SECURITY INCIDENT" in the subject.
- **External reporting:** sellers, buyers, partners and researchers can report suspected vulnerabilities or incidents to **hello@scan2tray.com**; the address is published on **scan2tray.com/security** and is monitored daily. Good-faith reports are acknowledged within 2 working days.
- **Automated signals:** database health alerts, rate-limit and abuse alerts, and dependency vulnerability alerts are delivered to the Incident Lead's mailbox.
- **Incident record:** every incident gets a written timeline (detection time, actions, decisions, evidence) kept for at least three years.

## 4. Response process

| Phase | Target | Actions |
|---|---|---|
| 1. Detect & triage | Within 1 hour of report | Incident Lead confirms whether it is an incident, assigns a severity (Critical: personal data or credentials exposed / service down; High: likely |

| | | |
|---|---|---|
| | | exposure or partial outage; Medium: contained, no exposure; Low: policy breach without impact) and opens the incident record. |
| 2. Contain | Immediately, before full analysis | Revoke or rotate affected credentials, keys and marketplace tokens (per shop where possible); block abusive sources at the firewall; isolate or wipe compromised devices; take an affected component offline if needed to stop harm. Preserve logs first. |
| 3. Assess | Within 24 hours | Establish what happened, which data and which sellers, buyers or partners are affected, the root cause, and whether personal data was involved. |
| 4. Notify | See section 5 | Inform affected parties with plain facts: what happened, what data, what we did, what they should do. |
| 5. Recover | As soon as safe | Restore service from clean builds or backups; verify integrity; re-enable access progressively; monitor for recurrence. |
| 6. Review | Within 10 working days of closure | Post-incident report: timeline, root cause, what worked, what didn't, and concrete corrective actions with owners and dates. Update policies and controls accordingly. |

## 5. Notification obligations

- **Sellers:** affected sellers are notified without undue delay by email once facts are confirmed, and in any case within 72 hours of confirming a personal-data breach.
- **Regulator:** where personal data is involved and the breach is likely to result in a risk to individuals, the UK Information Commissioner's Office is notified within 72 hours as required by UK GDPR (and the relevant EU authority for EU data subjects).
- **Marketplace partners:** where a partner's platform, data or API credentials are involved, that partner (including TikTok Shop through its Partner Center channels) is notified promptly and in line with its partner terms, and the affected app authorisation is revoked or rotated.
- **Suppliers:** hosting, payment or email providers are engaged where the incident originates with or affects their service.
- **Public disclosure** is decided by the Incident Lead once affected parties have been informed.

## 6. Readiness

- Production credentials, keys and marketplace tokens can be rotated or revoked individually without a full redeploy.
- Database backups are taken daily and a restore is tested at least annually.
- Staff are briefed on this policy on joining and at each annual review; the process is walked through against a realistic scenario at least once a year.

## 7. Review

Reviewed with the Information Security Policy at least annually and after every Critical or High incident.